UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,007	04/15/2004	Ryan James Berg	286685.124US1	7251

23483 7590 11/29/2006

WILMER CUTLER PICKERING HALE AND DORR LLP
60 STATE STREET
BOSTON, MA 02109

EXAMINER	
KISS, ERIC B	

ART UNIT	PAPER NUMBER
2192	

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/825,007	BERG ET AL.	
	Examiner	Art Unit	
	Eric B. Kiss	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 19, 2006, has been entered.

Claims 1-22 are pending.

Response to Amendment

2. Applicant's amendments to the claims appropriately address the rejection of claims 1-22 under 35 U.S.C. § 101. Accordingly, this rejection is withdrawn.

3. Applicant's amendments to the claims appropriately address the rejection of claims 1-22 under 35 U.S.C. § 112. Accordingly, this rejection is withdrawn.

Response to Arguments

4. Applicant's argument that Viega "teaches away" from using compiler techniques is not persuasive. Viega teaches a modified parser while recognizing that "real" parsing has advantages over their system ("However, without 'real' parsing we cannot accurately determine all identifiers that are lexically used as variables." (section 4.1; see also section 8)). Applicant's apparent suggestion that Viega "teaches away" from the use of compiler techniques in general is simply untenable (*e.g.*, Viega describes, *inter alia*, a static analysis tool including a lexer).

5. Applicant's other arguments are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-16 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over David Wagner, et al., "A First Step Towards Automated Detection of Buffer Overrun Vulnerabilites," Proceedings of the Network and Distributed System Security Symposium, Feb. 2000, (prior art of record; hereinafter *Wagner et al.*) and David Larochelle and David Evans, "Statically Detecting Likely Buffer Overflow Vulnerabilities," Proceedings of the 2001 USENIX Security Symposium, Aug. 2001, (prior art of record; hereinafter *Larochelle/Evans*).

As per claims 1, 15, and 16, *Wagner et al.* discloses analyzing variables in source code in the context of at least one of the inherent control flow and inherent data flow and creating models therefrom in which each model specifies pre-determined characteristics about each variable (see, for example, section 1.1); using the variable models to create models of arguments to routine calls in the source code (see, for example, sections 1.1 and 3); using the argument models in conjunction with pre-specified criteria for the corresponding routine calls to determine whether the routine calls possess vulnerabilities as a consequence of the arguments and known routine behavior (see, for example, sections 1.1 and 4); and generating a report that identifies the vulnerabilities (see, for example, Fig. 5). *Wagner et al.* further discloses a viewable report (see, for example, Figure 5).

Although *Wagner et al.* discloses a flow-insensitive technique, flow-sensitive techniques are specifically contemplated (see, for example, *Wagner et al.* at p. 5, col. 1 (describing flow-insensitive analysis); p. 10, col. 2 (acknowledging the benefits of a flow-sensitive approach"

"One way to reduce the number of false alarms requiring human attention is to trade off time for precision . . . . For example, we could envision moving to a flow-sensitive to context-sensitive analysis."; Table 2 (showing the expected reduction in false alarms from improvements to the analysis involving flow- and context-sensitive analyses)). Further, *Larochelle/Evans* teaches a vulnerability detection system that employs such a flow-sensitive approach (see, for example, *Larochelle/Evans*, section 5 (data flow) and section 6 (control flow)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the use of flow-sensitive techniques with the vulnerability detection techniques of *Wagner et al.* and *Larochelle/Evans*. One would be motivated to do so to reduce the number of false positives (*Wagner et al.*, p. 5, col. 1, and Table 2).

As per claim 2, *Wagner et al.* further discloses the models specifying the memory size of a variable (see, for example, sections 1.1 and 3).

As per claim 3, *Wagner et al.* further discloses the models specifying the data size of a variable (see, for example, sections 1.1 and 3).

As per claim 4, *Wagner et al.* further discloses the models specifying whether the variable is a null terminated string or not null terminated string for variables of string value type (see, for example, sections 1.1 and 3).

As per claim 5, *Wagner et al.* further discloses the models specifying the type of memory of a variable (see, for example, sections 1.1 and 3).

As per claim 6, *Wagner et al.* further discloses the models specifying the value of a string for variables that are of a string value type (see, for example, sections 1.1 and 3).

As per claim 7, *Wagner et al.* further discloses the models specifying the origin of the data for a variable (see, for example, sections 1.1 and 3).

As per claim 8, *Wagner et al.* further discloses the models specifying characteristics of variable arguments (see, for example, sections 1.1 and 3).

As per claim 9, *Wagner et al.* further discloses the models specifying characteristics of expression arguments (see, for example, sections 1.1 and 3).

As per claim 10, *Wagner et al.* further discloses the models being specified as lattices (see, for example, sections 2 and 3).

As per claim 11, *Wagner et al.* further discloses the lattice values including at least one of a value to represent no knowledge, a value to represent inconsistent knowledge, and a value to represent a refinement of knowledge (see, for example, sections 2 and 3).

As per claim 12, *Wagner et al.* further discloses the value to represent a refinement of knowledge including values to specify a range of specific values (see, for example, sections 2 and 3).

As per claim 13, *Wagner et al.* further discloses the pre-specified criteria for the corresponding routine including rules about the semantic behavior of the routine (see, for example, sections 1.1 and 3).

As per claim 14, *Wagner et al.* further discloses the vulnerabilities being buffer overflows (see, for example, section 1.1).

Regarding claims 20-22, *Wagner et al.* fails to expressly disclose identifying the location in the source code listing where the vulnerability occurred. However, *Wagner et al.* clearly indicates that such a feature would be desirable (*Wagner et al.* at p. 11), and *Larochelle et al.*

teaches providing such vulnerability location information (see, for example, the representative output in section 4.1 of *Larochelle et al.*, describing a vulnerability (possible out-of-bounds store) at line 1112 of source code file *ftpd.c*). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to provide such a vulnerability location feature as taught by *Larochelle et al.* in order to gain the advantage of knowing which statement in a source code file is at fault for a particular vulnerability.

8. Claims 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Wagner et al.* and *Larochelle/Evans* in view of John Viega, et al., "ITS4: A Static Vulnerability Scanner for C and C++ Code," 2000 (art of record; hereinafter *Viega et al.*).

Regarding claims 17-19, *Wagner et al.* fails to expressly disclose using a database having computer readable information about a predefined set of source code routine calls, said information specifying one or more conditions that present a vulnerability during execution of the routine call; and using the database to retrieve information for a corresponding routine call to check for the specified condition to see whether the routine call presents a vulnerability. However, *Viega et al.* teaches that it is beneficial to use a database of vulnerabilities, including a description of possible problems, hints on how to tell if there really is a problem, and suggested fixes, and to compare a token stream based on source code with the database to detect vulnerabilities (see, for example, sections 2, 4.1, and 4.2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to use such a database to facilitate the detection of vulnerabilities. One would be motivated to do so to maintain expert knowledge regarding vulnerabilities in a format that can be easily modified.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Eric B. Kiss whose telephone number is (571) 272-3699. The Examiner can normally be reached on Tue. - Fri., 7:00 am - 4:30 pm. The Examiner can also be reached on alternate Mondays.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Tuan Dam, can be reached on (571) 272-3695. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature should be directed to the TC 2100 Group receptionist: 571-272-2100.

Eric B. Kiss
November 27, 2006